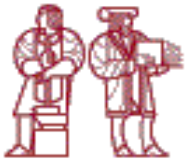
MIT-NED-EDF–1999-01

Review of International Activities in Accident Management and Decision Making in the Nuclear Industry

by
Curtis Smith, Emanuele Borgonovo, and George Apostolakis
Massachusetts Institute of Technology

May, 1999



Abstract

This report provides an overview of available international work related to accident management, decision making, and the use of formal techniques in response to events at nuclear power plants. Within this body of research, our efforts focused on evaluating off-normal events for both pre and post-core-melt situations. As part of the review, we first provide an overview of background material including probabilistic safety assessment and decision analysis. We provide, via examples and applicable references, a look at current international activities in accident management. In the report, these activities are divided into two types of actions, prevention and mitigation, in order to contrast the differences between the two responses. We conclude that accident management must be considered as a decision-making problem with sequential decisions under uncertainty. Formal techniques such as influence diagrams have revealed themselves as an appropriate tool to perform such an analysis. Lastly, an annotated bibliography of relevant published literature is provided.

Contents

1. Introduction

Since nuclear power plants (NPPs) are complex technological systems, a variety of events or occurrences normally happen during the standard course of operation. These events span the gamut from simple, non-safety-related component outages to complex plant transients that might lead to damage of the reactor core. To help defend against these events, many plants have well-defined standard operating procedures (SOPs). For normal conditions, SOPs are rigorously defined and are an accepted part of plant operations. Training is provided to the operators[†] and, on the average, a high level of efficiency has been achieved by the nuclear industry.

For upset conditions, Emergency Operating Procedures (EOPs) are normally available and are integrated with the SOP. This integration varies in different ways depending on the country and on the facility. Training is also provided to the operators to comply with the most commonly encountered problems (usually through simulator training). Nevertheless, management of personnel, operator actions, and decision making during abnormal situations is a critical task and raises specific issues that deserve the attention of the nuclear industry.

From a theoretical point of view, accident management is a sequential decision problem involving a decision maker in the presence of uncertainty. Following an initiating event or due to upset plant conditions, the "decision maker"[‡] must take action to restore normal plant operations. For the recovery actions to be successful, the problem must be diagnosed correctly and the right strategy must be adopted. Uncertainty may exist about the exact plant status at the time of the off-normal event as well as on the initiating event until the moment of its diagnosis. Human actions influence the progression of the incident and can make the accident worse if proper guidance is not provided. Uncertainty, therefore, is one of the major issues in accident management since it is ingrained in both the "problem and the solution" taken during an accident.

Within the context of uncertainty, we are faced with two categories defining the type of uncertainty, aleatory and epistemic (Apostolakis, 1995). Aleatory uncertainty characterizes the randomness of events. For example, we do not know when a transient such as a loss of off-site power (LOSP) will occur. Or, given a demand on a safety system, will the particular system start successfully? And, will the operator diagnose the safety system problem correctly and take the corresponding recovery action? We could go on with a long list of random events and phenomena, each of which can be more or less adequately modeled via an aleatory model of the

[†] In the USA, personnel in Nuclear Power Plants spends around 25% of their time in training.

[‡] The decision maker could be represented by a person or a hierarchy of people. For the sake of simplicity we will refer to it as simply the decision maker, allowing us to discuss this entity later in our work.

world (MOW) framework. Now, for the MOW, a lack of data normally makes it impossible to determine an exact numerical value for the parameters of the MOW. Consequently, epistemic uncertainty will need to be introduced (Apostolakis, 1995). As a result of these two uncertainties, important quantities in the accident sequence can not be determined exactly. For example, timing and magnitude of the physical phenomena in an accident sequence cannot be established with absolute precision, especially if we refer to post-core-melt conditions. Consequently, the allowed grace times for procedural steps will be known only within a certain range, complicating the choice and allocation of operator action. The credibility (and feasibility) of an accident management strategy therefore has become an issue.(Dougherty 1992) We will summarize some of the methodologies that have been studied to ensure a comprehensive strategy evaluation.

After the Reactor Safety Study and the Three Mile Island accident in the U.S., a large effort has been put into the study and development of severe accident management strategies, especially with regard to their technical aspects. However, it has not been difficult to realize that, although a strategy is successful from an engineering point of view, this does not mean that it is guaranteed to be feasible. Other factors can pose doubts on the success of the strategy; these factors include the complication of the procedure or insufficient action times that increase the probability of human error. Therefore, beside traditional engineering analysis, methods have been developed to account for the man-machine interface. These have brought to accident management the consideration of issues as a dynamic decision problem. Tools of the decision analysis domain , such as influence diagrams and decision trees, have revealed themselves suitable to a more comprehensive analysis. However, the great deal of work that has taken place in severe accident management has been accompanied by a criticism. It is known that severe accident management deals with events that occur after core melt. From many sides, it has been claimed, that due to the very low probability of such events, resources could be better allocated in trying to refocus on plant availability, trip reduction, and incident preparedness (Dougherty 1992). Nonetheless, a significant effort has been put in the study of EOPs and in the development of operator supporting tools. But, the need still remains for an overall approach to the complex problem of accident management.

The objective of this document is to provide an overview of existing international work related to accident management, decision making, and the use of formal techniques in response to events at nuclear power plants. The context of events in this document covers both pre and post-core-melt scenarios. The layout of the document is to provide a general overview of existing formal techniques of interest including those from probabilistic safety assessment (PSA) and decision analysis (Section 2). Then, the document provides an overview of current international activities in accident management via discussed examples and related references. These activities are divided into two types of management actions, prevention (Section 3) and mitigation (Section 4). Following the activities discussion, conclusions are presented. Lastly, at the end of this document is a list of all references used in the text. In addition to the references, Appendix A provides an annotated bibliography of relevant published literature.

2. Background Concepts

2.1 Scope and Purpose of a PSA

During the operation of a nuclear power plant, conditions exist that alter the risk of operating the facility. These conditions (or events) that result in a change, where "change" can be either an increase or decrease in risk, fall under three general categories. First, plant activities dictate that certain components will be incapable of performing their desired functions at certain times during operation. Examples of these activities that incapacitate components include preventative maintenance and testing (both scheduled activities), corrective repairs to failed components (an unscheduled activity), and Technical Specification actions such as either entering a Limiting Condition of Operation to replace a component or performing specified functional tests (these activities could be either scheduled or unscheduled). Second, improper plant design or maintenance could result in an unintended reduction in plant or component reliability, potentially over long periods of time. Examples of these reductions in plant reliability include faulty component design such as undersized valve motor operators and insufficient fire-barrier protection or faulty component restoration and testing after a maintenance activity. Third, initiating events that occur during operation cause challenges to plant systems and operators. Examples of these events include losses of off-site power, miscellaneous plant transients, and loss-of-coolant pipe breaks.

To address the risk of operation, the methodology of PSA (or probabilistic risk assessment, PRA) has been accepted in the nuclear power generation industry. Within a full-scope PRA, the analysis (or logic models and supporting calculations) are generally artificially subdivided into three parts, or "levels." A high-level depiction of the three levels of PSA is shown in Figure 1. Level 1 addresses the quantification of sequences leading to core damage. This involves the determining events that challenge plant operation (i.e., initiating events). Then, in response to the initiating events, the plant response must be identified. This identification is modeled through the use of fault trees and event trees. From the fault trees and event trees, the accident sequences are obtained. Then, the Level 2 PSA evaluates subsequent plant responses to the core damage event. And then finally, the Level 3 analysis addresses the ultimate consequences to the public from the core melt event. These "levels" are discussed in additional detail in Section 2.2.

The use of a PSA varies. Some PSA were developed in response to specific regulatory requirement while other were developed to address plant-specific risk issues. Current applications of PSA include utilization for plant operations (e.g., a "risk monitor"), screening of generic safety issues, and the allocation of resources.

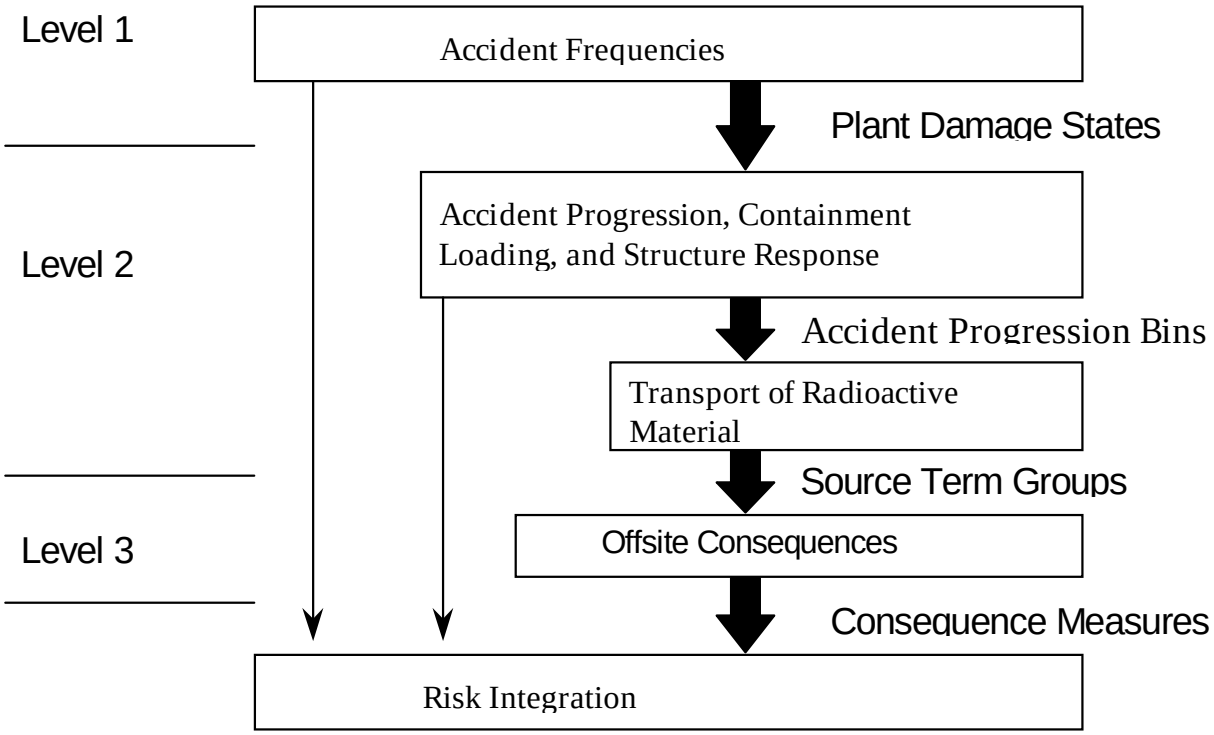


Figure 1. Illustration of the three PSA "levels" that are used to sub-divide the analysis.

Typical PSAs that are performed for nuclear power plants focus on initiating events that occur "internal" to the plant (so-called internal events) that happen at power. A similar type of analysis for events that happen while the plant is in a shutdown or low power mode may be available. In addition, a plant PSA may include "external" initiating events (e.g., earthquakes, fires, floods, severe weather). For the work to be performed for this project, the analysis and development will focus on internal events for full power operations due to the availability of an applicable PSA model.

2.2 The Three PSA Levels

For the Level 1 analysis, fault trees are utilized to determine system response. This response is characterized as a system failure probability. Then, these fault trees are tied to the event tree logic models (which characterize the general plant response to initiating events). From the fault tree and event tree modeling, the accident sequences are determined. This modeling is represented in Figure 2 below.

Initiating Event	Reactor Protection System	Feedwater	Residual Heat Removal	#	END-STATE-NAMES
IE	RPS	FEED	RHR		

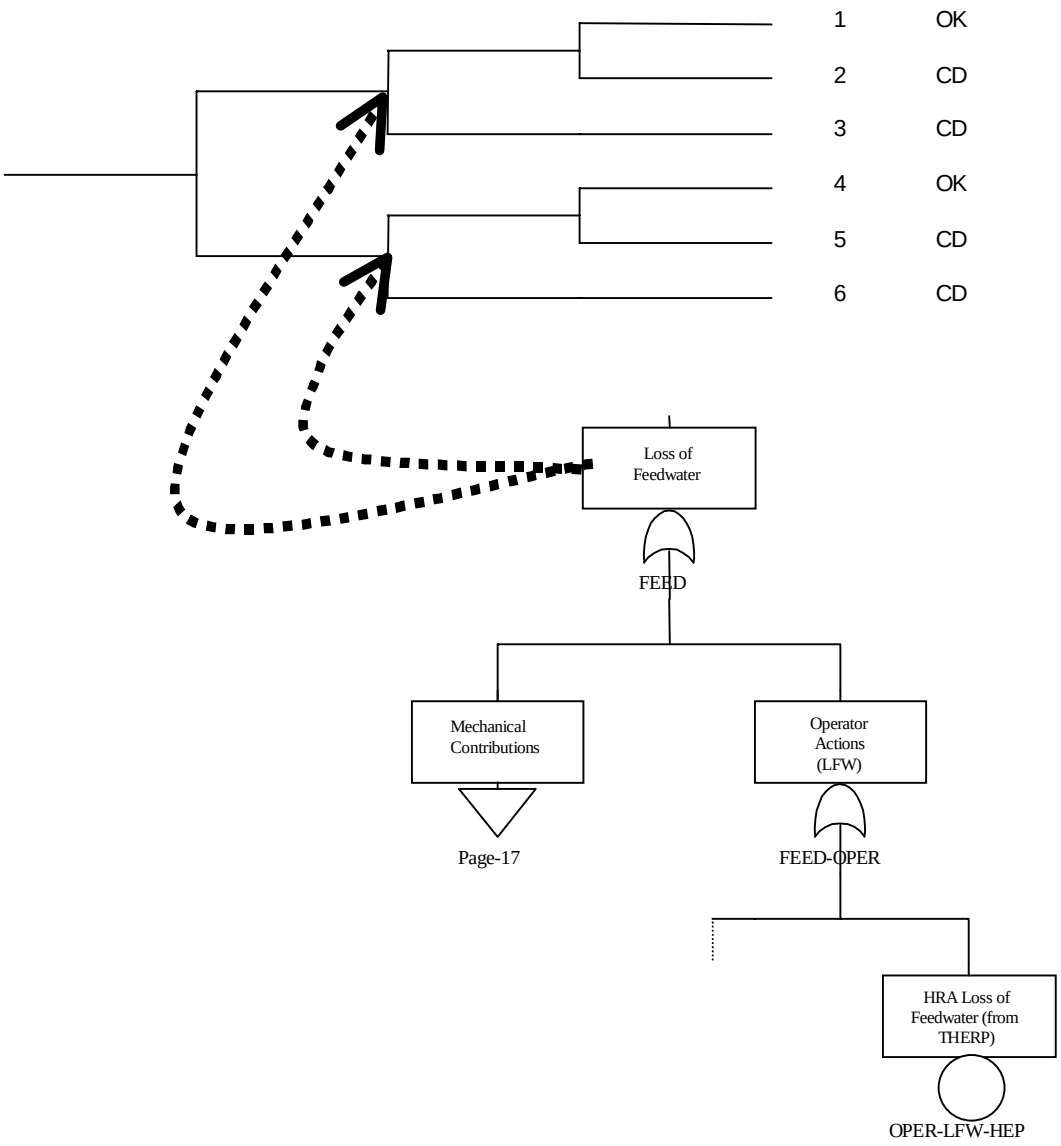


Figure 2. A representation of the accident sequence modeling from the Level 1 PSA.

From the Level 1 accident sequences (the 2, 3, 5, and 6 from Figure 2), the core damage frequency can be quantified. Further, we could gather "like" accident sequences into what are called plant damage states (PDS). In many PSAs, the PDS is normally comprised of up to eight characteristics and is intended to define the plant status at the onset of core damage. This PDS "vector" yields the boundary conditions for what is called the Level 2 source term event tree (STET). Note that since the PDS gives pre-core damage information, the development of the part of the model would be of interest in the accident management framework.

Progressing through the accident scenario we come to the STET. The STET is really what is thought of when a Level 2 model is discussed. This model represents the accident progression from the onset of core damage to the release of radioactive materials to the environment from containment. Note that important events in this part of the analysis include:

- The mode of vessel breach
- The performance of containment systems in mitigating the radioactive release
- The mode of containment failure

In a Level 2 analysis, the Level 1 PDSs are aggregated to be used as the initiating events to the STET. Traditionally, the approach for quantifying the branch probabilities of the STET relies on the quantification of the NUREG-1150-type accident progression event trees (APETs). In some cases, quantification of a STET top event may be represented by a fault tree that reproduces the logic in the APET leading up to that particular summary event. In other cases, the STET event may be determined by simply assigning split fractions (these split fractions are currently quantified using codes like EVNTRE and PSTEVNT). Then, following the Level 2 event tree models, the Level 3 consequences, the radioactivity release fractions, are determined. Consequences are calculated using computer codes like MACCS.

A simplified diagram illustrating the analysis "flow" from Level 1 through Level 3 analysis is shown in Figure 3. This figure is useful since it allows an analyst to see, at a particular PSA Level, what are the calculations and outputs that are to be expected. Thus, for an accident management approach that focuses on pre-core damage, items of interest include: the initiating events, the event trees (accident sequences, success criteria), and the system fault trees (component failures, operator actions).

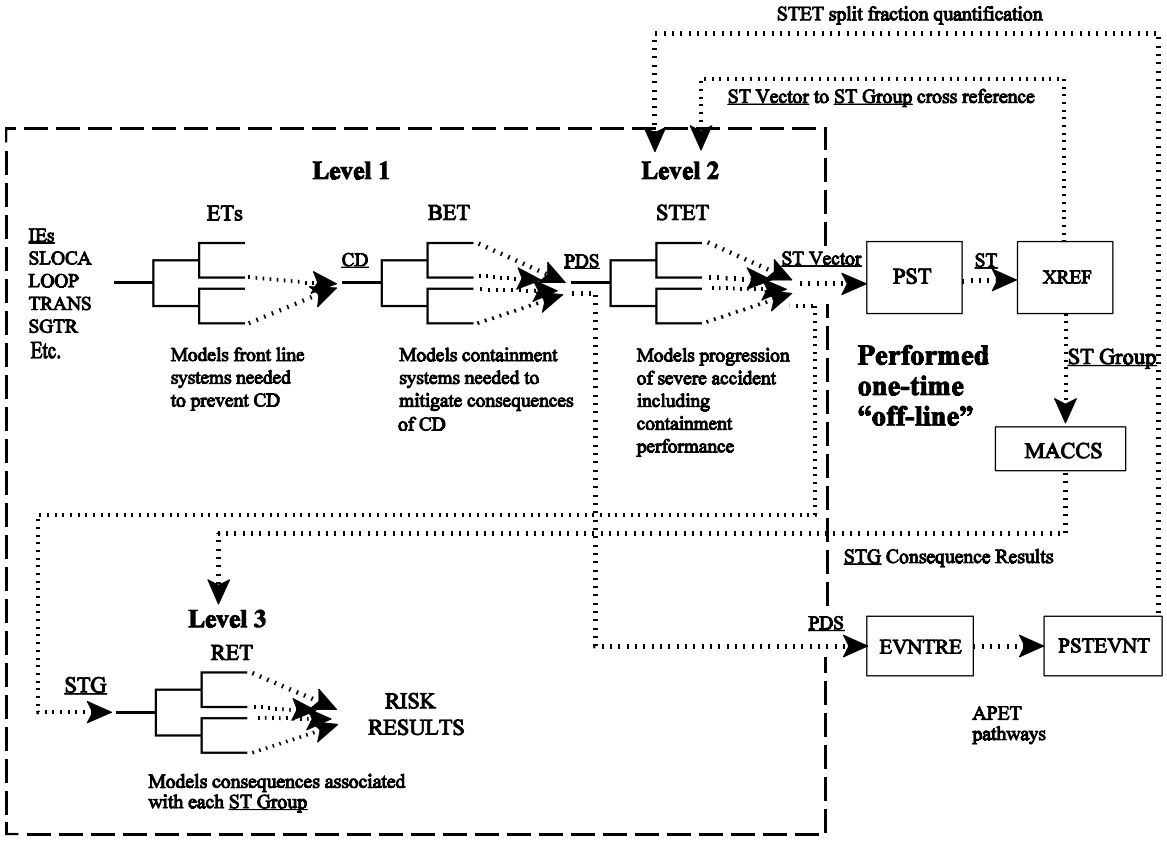


Figure 3. The analysis "flow" for the three levels (Level 1, 2, and 3) of a typical PSA.

If the accident management analysis were to focus on Level 1 issues, the resulting problem definition would be substantially smaller than that for a Level 2 or Level 3 focus. But, this does not imply that the problem is trivial. Indeed, the problem of decision making during accident situations leading to core melt is complicated. Fortunately, tools like influence diagrams, decision trees, and PSAs decompose this (complicated) issue into manageable and tractable pieces. For example, Figure 4 provides an overview of the most relevant analysis parts that are introduced in a Level 1 PSA. Decision making within a Level 1 scenario would most likely have to address most, if not all, of the parts identified in the figure.

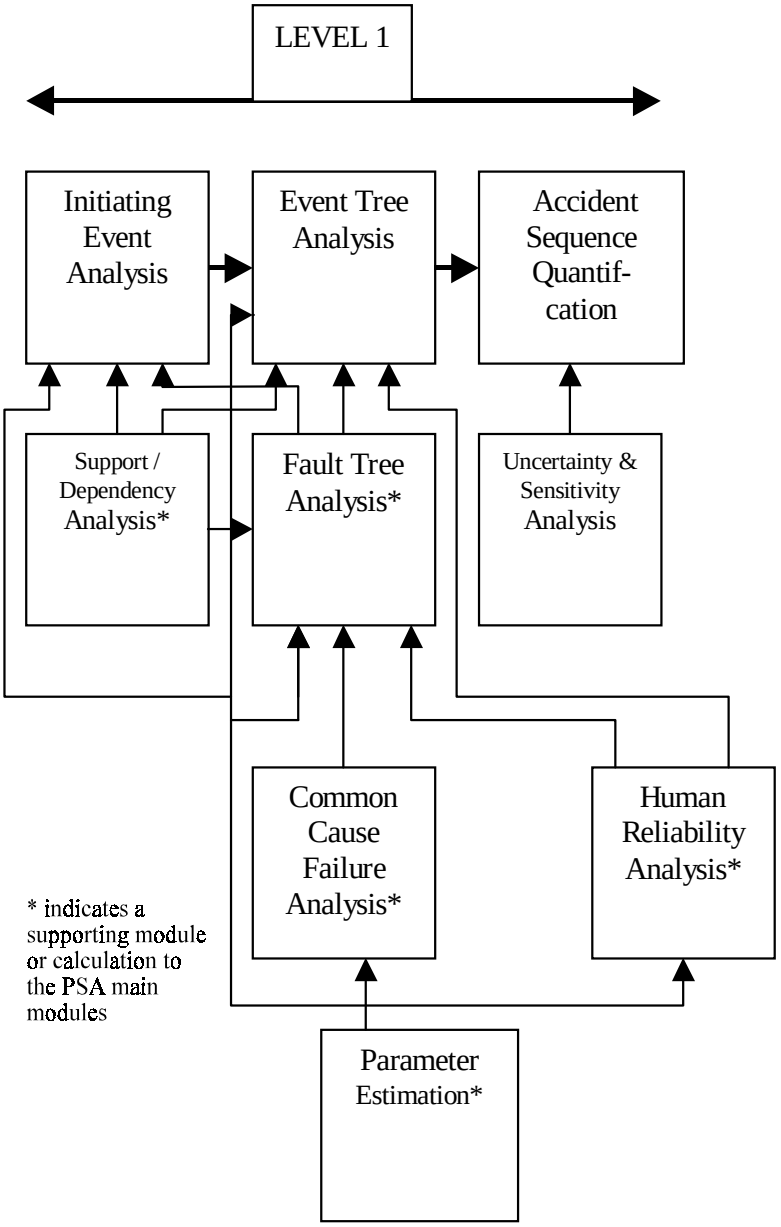
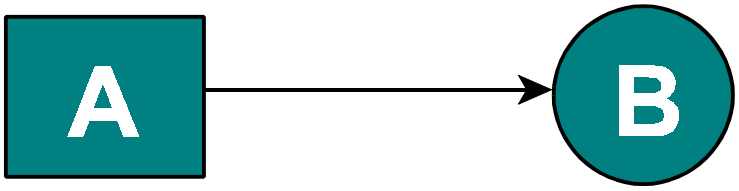


Figure 4. Analysis items that are traditionally part of the Level 1 PSA.

2.3 Formal Decision Analysis Tools

The two most important tools in formal decision analysis are the influence diagram and the decision tree. While these tools have not seen wide use in the nuclear industry, they are considered to be a vital part of any strategy of decision-making. Consequently, their use in accident management, while demonstrated in for simplified cases, will ultimately be needed (Catton and Kastenburg, 1998; Jae et al., 1993).

First, a brief discussion of influence diagrams and then decision trees will be presented (Jae and Apostolakis, 1992). Influence diagrams are a graphical method of describing dependencies between random events and decisions. For example, the simple influence diagram



represents that the probability of the aleatory event B depends on the decision A.

For another example, let us suppose that at a certain time, during operation of a nuclear plant, an non-threatening event happens. The owner/operator faces the question of whether or not to take action in response to the event. If a response is required, then the next decision is what type of response to make. This response could be any number of possible actions such as shutting the plant down, continuing operation at a reduced power level, monitoring key components more closely, or a combination of these actions. For this example, a generic influence diagram is shown in Figure 6. The nodes before the decision node reflect the knowledge of the decision-maker at the time of the event. The decision-maker has to take into account several elements, which are represented by the "general information" and "plant condition" nodes. Aleatory events are represented in the "development" part of the influence diagram. The ultimate decision outcome is represented by the "utility" node.

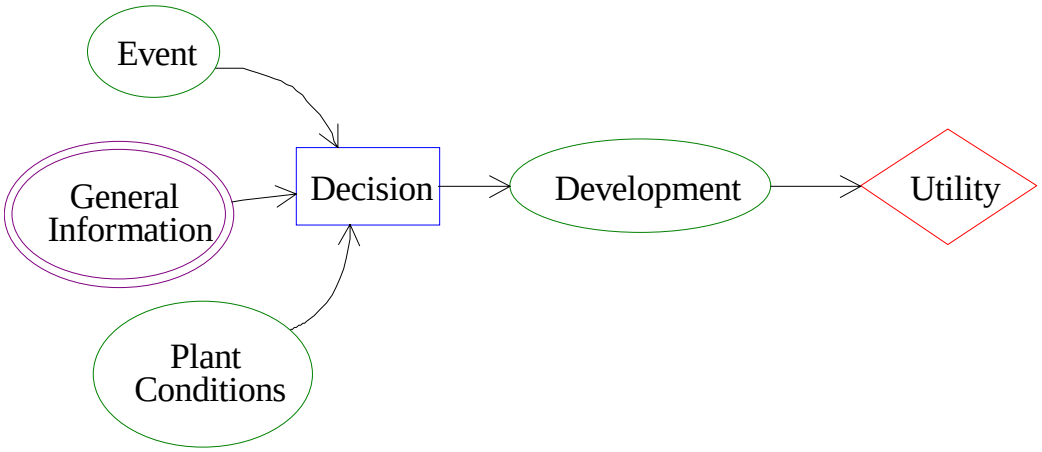


Figure 5. A general influence diagram giving a overview of the structure of the decision problem.

An influence diagram allows an analyst to present an overview of a particular problem in a high-level fashion. From this diagram, the intricacies and influence that are a part of the decision making process are readily apparent. Further, the influence diagram can be used to numerically evaluate decision making choices through the use of decision trees. A representation of a decision tree is shown in Figure 7. Circular nodes on the tree represent chance events, i.e., aleatory events.

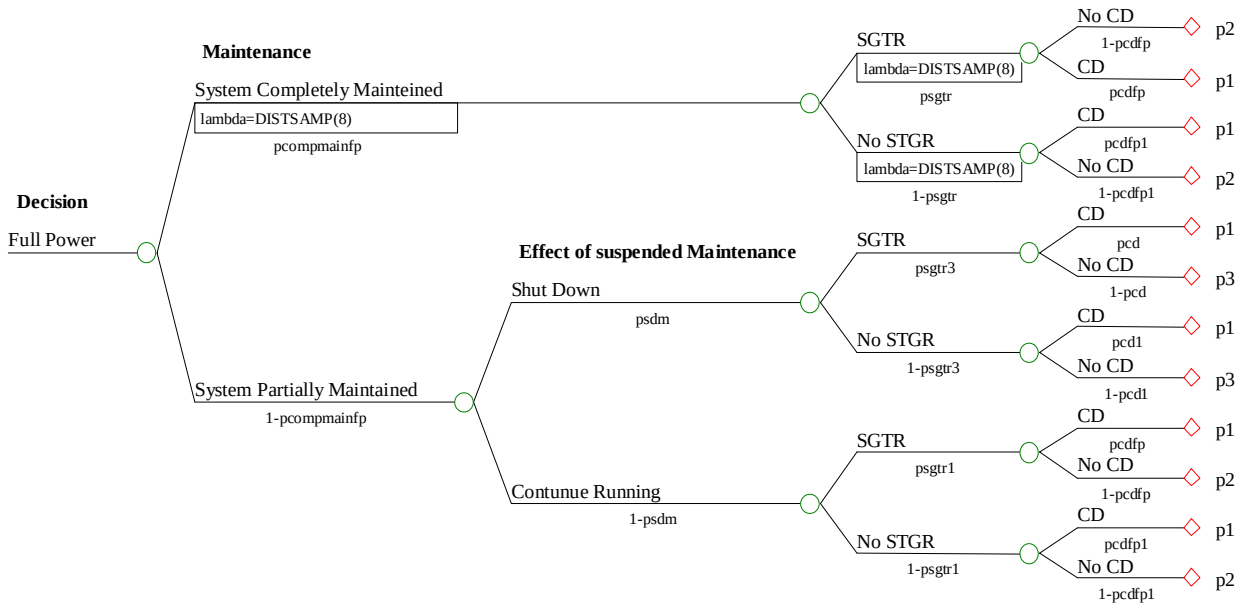


Figure 6. Representation of a decision tree structure.

Note that while decision trees look similar to their PSA counterpart, the event tree, they are two different models. Both incorporate probabilistic chance nodes, hence their similarity. But the decision tree "traces" the outcome of a decision or decisions and incorporates that conditional result of any decisions (e.g., cost of modification, revenue stream after changing product) while an event tree yields the probability or frequency for a certain, specified outcome (e.g., early core damage, plant in hot standby). Thus, an event tree is a decision tree without any decision nodes.

2.4 Other Relevant Technologies

We have already mentioned the fact that operational events leading up to and going beyond core damage are complicated and require sophisticated analysis techniques. Included in these techniques are the PSA methods and decision analysis methods presented in the previous sections. In addition to these methods, other analysis techniques are available and may be suitable for use in a decision framework for accident management strategies. Included in these potentially useful techniques are:

- Dynamic PSA tools like dynamic event trees.
- Human reliability analysis tools such as MERMOS, THERP, and ATHEANA.
- Deterministic thermohydraulic calculation tools

The remainder of this document provides an overview of current international activities in accident management via discussed examples and related references. These activities are divided into two types of management actions, prevention (Section 3) and mitigation (Section 4).

3. Accident Prevention

As we mentioned in section 1, activities in the field of accident management have generally fallen into one of two categories, prevention or mitigation. The term "accident prevention" defines the set of actions intended to assure core cooling and containment integrity. These actions presume the use of the best possible application of existing equipment, even if operation is beyond licensed conditions. The term "accident mitigation" defines the set of actions intended to avoid containment failure and radiation release following core melt. Again, these action presume the use of all the available equipment. Severe accident management is the term which groups all the studies and activities done in the area of post-core melt operations. Note that during the entire review of existing international research, we did not find any instance where the term "accident management" referred exclusively to pre-core damage events. Consequently, for this project, we may want to avoid the use of the term "accident management" in the context of Level 1 PSA in order to avoid confusion.

Preventive accident management strategies are based on EOPs. In this context, it is common to distinguish between "event-based" EOPs and "symptom-based" EOPs.[†] How these procedures are defined and utilized varies from country to country. For example, in Germany, once the plant safety functions reveal an abnormal condition, the particular type of EOP that is used is determined on whether the initiating event is identified. If the initiating event is identified, event-oriented procedures are followed, otherwise symptom-based procedures will be used. This concept is illustrated in Figure 8.

One of the limits of event-based EOPs is that they require operators to correctly diagnosis the scenario before they respond to the event. Correct diagnosis is often not an easy or a quick process. Nevertheless, timely action is crucial in the actuation of an accident management strategy. Hence symptom-based procedures have been introduced to complement traditional EOPs in case diagnosis is not performed (or is not done at all) in a sufficiently short time. These EOPs are based on certain critical plant parameters. From these parameters, action has to be taken when one or more of these parameters reach or go beyond a certain threshold value.

[†] TMI demonstrated that the diagnosis of an initiating event may not be an easy task, and delay in taking action could be lethal to the plant. Therefore symptom-based procedures were introduced to support the event oriented procedures. A fundamental concept here is that critical plant functions, such as core cooling, must be always assured, independently on the initiating event.

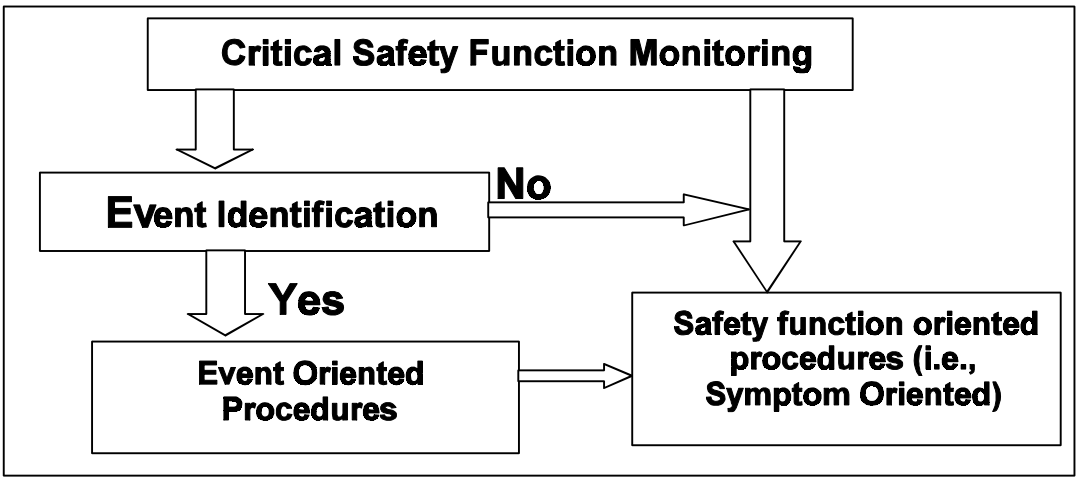


Figure 7. Monitoring of plant safety functions can reveal an abnormal plant condition; if the initiating event is identified, event-oriented procedures are followed, otherwise symptom-based procedures will be used (Roth-Seefrid et al., 1994).

Now, we will illustrate additional research on prevention features with examples available in the international literature about activities and studies in the area of accident prevention.

First, the Netherlands Energy Research Foundation ECN has looked at accident management from a decision framework point of view. This research has been in collaboration with Delft University. Researchers at Delft University looked at operator actions and timing considerations for accident scenarios (only Level 2 though). This analysis did not preclude Level 1 considerations, but it was simply deemed to be outside the scope of analysis. The novel aspect of the work was to formally incorporate both decision trees and influence diagram techniques into the decision process using modern analysis tools. This overall framework that was presented provides a robust method for decision making. The goal of the accident management strategy part of this research was to prevent vessel failure, prevent containment failure, and minimize off-site release after core-damage.(Götz, 1996)

Also at Delft University, a project was performed to look at how fault trees can be used in operator decisions (and, hence, in decision making for accident management). The work centered around the construction of a "fault tree based real time operator support system." Included in this work was a decision support framework based upon component failures (via fault trees). An interesting aspect of this project was the attempt to incorporate *time* into the logic modeling (see Figure 9). The time factor is used to develop a ranked list of failure states and would, therefore, help to influence decision making.(Schouten, 1998) Note that this analysis was focused on a generic type of fault tree. Consequently, the methodology could be used for either Level 1 analysis or Level 2 analysis.

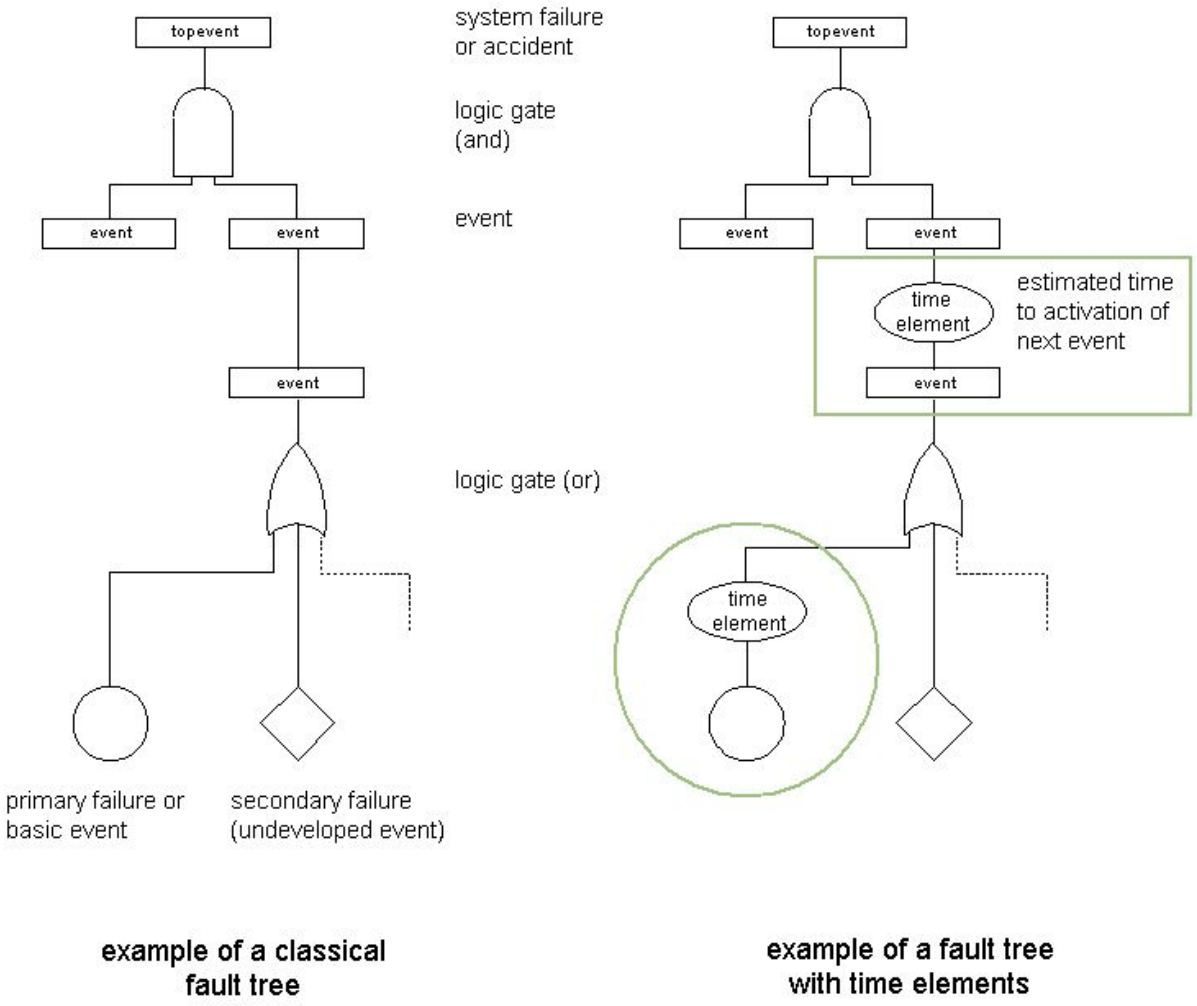


Figure 8. Modified fault tree incorporating the element of time. (from Schouten)

3.1 A German Accident Management Strategy Example

We know that one of the major changes in the way of considering risk for nuclear power plants was the Reactor Safety Study. Similar studies were performed later in other countries. In Germany, great importance was given to the results of the German Risk Study. One of the main results of this study was that the implementation of feed and bleed procedures would improved safety. Following an integrated PSA analysis, it was estimated that this strategy would reduced the core damage frequency of Siemens PWRs by a factor of 10. On this basis, the German Reactor Safety Commission decided to equip all pressurized water reactors with the capability of feed and bleed.

The bleed and feed strategy for German PWRs differs somewhat from the concept used in other countries, where depressurization of the primary system through the pressurizer valves is commonly intended. In Germany, bleed and feed is performed first on the secondary side, in case

of loss of heat sink. This is again a result of the German Risk Study: it was in fact noticed that Siemens PWRs suffered of a common cause failure mode on the secondary side that provoked loss of heat removal (Roth-Seefrid, 1994). Bleed and feed of the secondary side was studied as a possible accident management strategy and the results were very optimistic. Depressurization of the primary side is foreseen only as a second preference, when it is clear that the accident cannot be controlled by the secondary action alone.

With reference to the implementation of the feed and bleed strategy for German PWRs, we will now analyze the most important phases of the definition and implementation of an EOP.

Scenario — The first step in the implementation of a procedure is to define plausible scenarios that will require its actuation. In evaluating the efficacy of the feed and bleed procedure, two main scenarios were considered as starting points: a complete loss of feedwater injection due to mechanical pump failure or loss of AC power.

Initiation criteria — A strategy must be initiated if certain conditions are verified. These conditions are known as initiation criteria. For the feed and bleed procedure, the initiation criteria are displayed in Table 1. As it is possible to notice criteria, both the symptom oriented and the event oriented situations manuals have an entrance to the feed and bleed procedure.

Table 1. Initiation criteria for secondary and primary bleed and feed.

Initiating Criterion	Event oriented	Symptom oriented
Secondary bleed and feed	Loss of AC Power and Diesel Generators	SG -level low for 3 SGs
Primary bleed and feed	n/a	Fuel Temperature>340 °C

Operator actions — The third step is the definition of the required actions. Required actions are the set of tasks the operator must implement in order for the strategy to be successful. These tasks are customized through the analysis of the plant. In our example, the first action is to restore SG feedwater supply. Two alternative paths are provided to the operators:

- To make use of the large water inventory of the auxiliary feedwater tank (350Mg).

- To connect a mobile pump to the emergency feedwater heater in the emergency feedwater building . (A simplified diagram of the reactor is given in Figure 10).

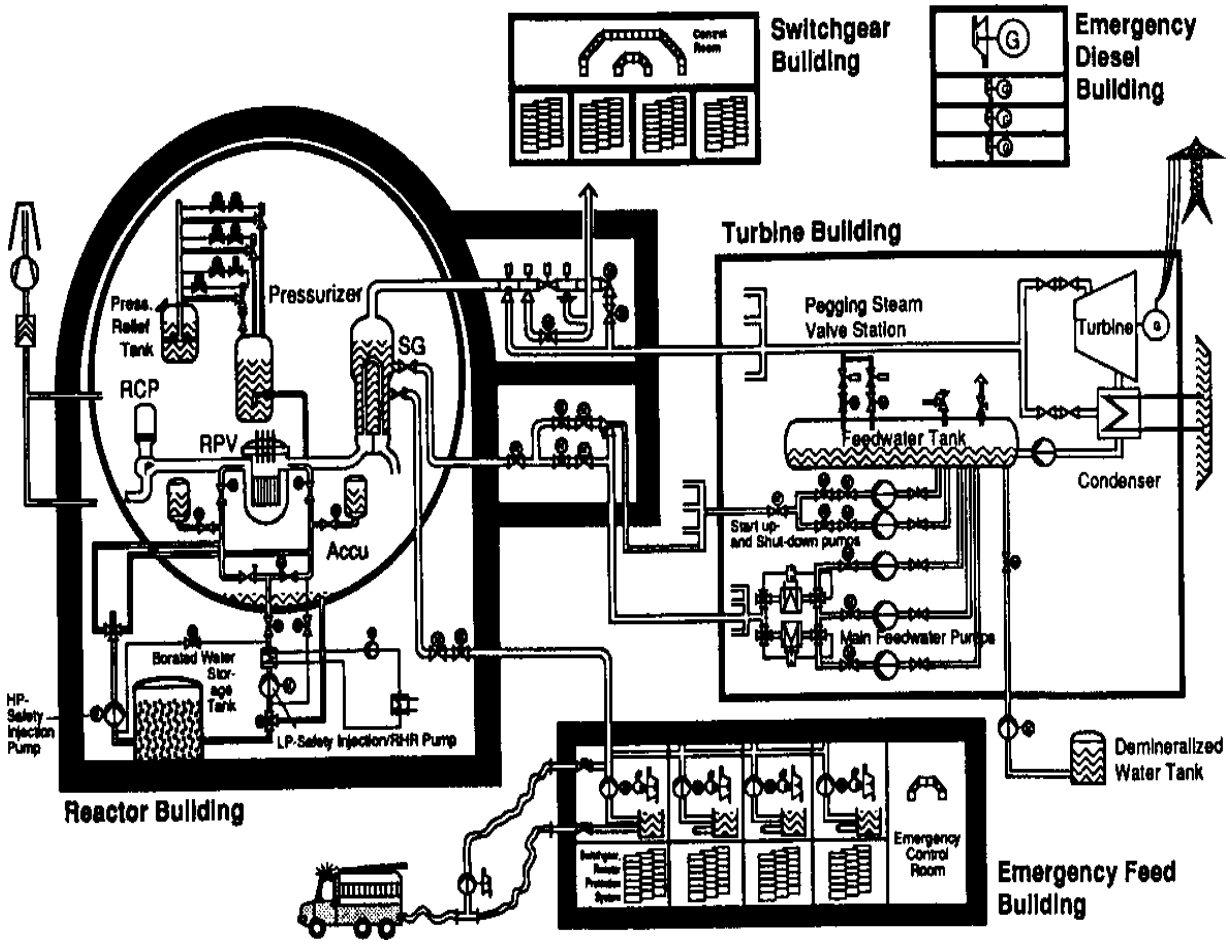


Figure 9. Simplified diagram of a Siemens PWR.

If strategy 1 is implemented, the operators should also heat the auxiliary feedwater tank to create a sufficient pressure drop to obtain adequate mass flow. This leads to a further complication; the pressurization of the auxiliary feedwater tank requires opening of a steam line from the SGs, which is equivalent to SGs depressurization. The secondary safety pressure monitoring system would interpret this low pressure as a secondary leak and would automatically isolate the SGs, rendering feed and bleed impossible. Up to 16 safety signals would have to be bypassed by the operators to successfully implement this procedure. From this consideration, it is easy to understand why human error has been found as the major contributor to the failure of the strategy.

Evaluation — The strategy is evaluated using tow results: the probability of "success or failure" and the overall benefit on the plant. In our example the failure probability[†] was estimated to be 1.2×10^{-2}, due mainly to human contribution, and the overall benefit was an estimated reduction of the core damage frequency by a factor 10 for existing plants and by a factor 4 to 7 for new ones.

Retrofitting — The last step in the implementation of the strategy is to identify possible plant design modifications to simplify actuation. In the example case, the problem was analyzed and modifications have been implemented by the facilities to deactivate the safety signals directly from the control room.

3.2 Dynamic PRA for Accident Management

Accident management deals with a dynamic process: transient events in nuclear power plants involve complex interaction between the reactor core, primary loop, balance of the plant, emergency safeguards systems, and operator activities.. Traditional static PRA event trees are not adequate to describe such a temporal evolution of events.

Methodologies based on dynamic PRA have been viewed as a natural step towards a more comprehensive way of evaluating Emergency Operating Procedures. The term "dynamic PRA" is used for a variety of methodologies, but essentially refers to modifications of the structure of the classical PRA to account for time-dependent effects (Hsueh and Mosleh, 1996). Dynamic effects can be grouped into two categories: long term effects (such as aging, environmental variations, plant design changes) and short time effects (such as time dependency of physical processes, time dependency of stochastic processes, operator response times). The

[†] This is the failure probability for the joint primary and secondary feed and bleed procedures. The results were obtained on PRA basis.

events occurring during an accident pertains undoubtedly to the second category, short time effects.

Features of a dynamic PRA are the following:

- Event sequences are represented by a “forward” branching tree where branching occurs in time, and therefore time is an explicit parameter of the model.
- Branching times are times in which an important characteristic of the system changes
- Event sequences are generated based on the rules describing the behavior of the various elements of the integrated model of the plant.

The event trees that result from such analyses are called Dynamic Event Trees (DETs). Depending on whether time is treated as a continuous or discrete variable, we will be dealing with Continuous DETs (CDET) or Discrete DETs (DDETs). An example of the application of DDETs is the Integrated Safety Assessment (ISA) Methodology which merges PSA and accident analysis techniques replacing the static ETs with DDETs. Here are the main steps of this methodology (Sanchez and Melara, 1996):

1. Identification of damage variables and definition of risk acceptable regions in a probability-damage plot
2. Initiating Event (IE) and initial state selection
3. Modeling the deterministic characteristics of the plant (plant dynamics modeling) including crew procedures
4. Modeling the stochastic characteristics of the plant (reliability modeling)
5. Event sequence generation
6. Analysis of the results and verification of the risk requirements.

ISA can be used to evaluate the effectiveness of a procedure accounting for the variation of the plant configuration with time due to the effect of crew operations. Three are the main elements of the model for the evaluation of EOPs:

1. A dynamic simulation model of the selected NPP and its safety features
2. A reliability model of the safety systems
3. A Handbook of Operating Instructions (HOI)

This last point deserves a further comment: during an accident, starting from an initiating event, the crew will take action. If the main purpose of the study is to analyze the effectiveness of the recovery actions suggested in the procedure, it is assumed that the crew will follow the instructions exactly as written. But, a software implementation of the reliability model of the plant in conjunction with the HOI will allow the computer-simulation of the accident sequence. The final result is an overall evaluation of the strategies, i.e., weaknesses in the procedures will be highlighted and links between different EOPs will be indicated when necessary to compensate for events that change the course of the accident. The critical point is to create sufficiently elastic EOPs to deal with all possible outcomes of an accident sequence.

Dynamic modeling of the plant behavior is not a simple task and adequate computer software must be developed. For example, the EOPs assessment in a Westinghouse PWR in Spain, required the merging of two computer codes: the DYLAM-TRETA code, a software package for the calculation of DDETs , and the HOI code that accounts for the EOPs interface. (The resulting code is the DYLAM-TRETA-HOI code) (Sanchez and Melara, 1996).

Another example of a methodology based on DDETs is the Accident Dynamic Simulation Methodology (Hsueh and Mosleh, 1996), in which plant thermal hydraulic behavior, safety systems response, and operator interactions are explicitly accounted for in an integrated analysis of the accident evolution. The corresponding code, the ADS (Accident Dynamic Simulator), uses an operator model that includes procedure-based behavior and several types of omission and commission errors. The potentialities of the code covers the following ranges:

- Evaluation of the impact of timing and sequencing of failure events on accident progression
- Creation of a test environment for study of a new generation of HRA models
- Creation of a test environment for the evaluation of the robustness of EOPs under different accident situation.

This last application of the ADS is quite similar to the DYLAM-TRETA-HOI code.[†]

[†] As can be noted looking to the references, the DYLAM-TRETA-HOI model has been studied and developed in Europe (Spain in this case) practically contemporarily to the ADS.

3.3 Depressurization in a Swedish ABB-BWR – The Importance of Operators

So far we have seen how PRA has been used to identify and evaluate EOPs. We have addressed the issue of the inadequacy of static PSA models for EOP evaluation. The hypothesis of no human error was made in order to evaluate recovery actions from a technical point of view. Suppose now that we have equipped our reactor with strict, technical procedure-based EOPs. We are still left with answering the question of whether the operators will follow the procedures, and if so, of whether they will be able to effectively perform their required actions (including diagnosis and decision). In view of these aspects, many authors consider the decision theoretical approach appropriate to a comprehensive evaluation of accident management strategies (Jae and Apostolakis, 1992; Dougherty 1992; Jae et al., 1993; Milici et al., 1995; Catton and Kastenberg, 1998; Svenson, 1998).

Decision theory treats choices under uncertainty (whether or not a certain events will happen, the consequences of a certain action) and in consideration of different goals (what are the goal of a certain decision, trade-off between different goals). To understand the features of this approach, we will follow the application to the depressurization sequence of a Swedish ABB BWR (Svenson, 1998).

First of all, let us look at the intrinsic decisional trade-off: suppose the scenario[†] is such that the shift supervisor faces the question of whether or not to go to depressurization[‡]. Although depressurization has a high probability of success and will probably ensure cooling, after depressurization the plant has to be stopped for several months for the necessary checks and repairs. Depressurization is a negative event for the plant and the decision maker has to be sure that the situation has been correctly diagnosed.

After the decision to depressurize, a *team* of operators will be at work; that is, the operators will not act as independent players, but will be part of an emergency organization. Issues such as team composition, team competence, and planning capacities are relevant to the overall strategy. In a realistic strategy evaluation, the role of the team and the organization should be taken into account.

Another feature that comes into the picture is the time allowed for the operators to perform their actions. The operators will have to make decisions under time pressure: the time available to

---

[†] The initiating conditions for depressurization are the following:

1- Low level in the reactor vessel (< 50 cm)

2- High pressure in the containment or rapid increase in pressure in the containment. The procedure can be manually or automatically initiated. Loss of feedwater and auxiliary feedwater are the initiating events.

[‡] Any reference to a specific plant was avoided in (Svenson, 1998).

initiate depressurization after loss of feedwater before core uncovery is estimated a 16 to 35 minutes depending on the thermal-hydraulic code used. In this time, the operators will have to take care of a reactor scram, make decisions about resource management (personnel allocation, for example) in order to restart the feedwater or the auxiliary feedwater system to avoid depressurization. These decisions are to be made in an abnormal environmental condition and they need to be continuously reassessed in light of new information.

Human reliability analysis models must be used to assess operators response. In this study, use of the traditional THERP (Swain and Guttman, 1983) methodology gave a result of a relative frequency of human error of 0.01. The important lesson from studies such as Svenson (1998) is that accident management is a *dynamic sequential decisional problem* and the success of a strategy relies heavily not only on the physical variables of the problem but also on issues such as team composition, emergency organization, and man- machine interaction.

3.4 Computer Packages as Operator Supporting Tools

It is evident from the above analysis that operator actions and responses during a sequence are crucial to the overall success of the accident strategy. One of the major problem areas is the quantity of information that the operator must absorb before making the decision. During an abnormal situation, the information overload and stress on the operator may severely affect his/her decision-making ability, right when it is required the most. Quick review and accurate diagnosis are very important to plant safety because relatively simple procedures can be implemented to correct the situation. A great deal of work has been done by the nuclear industry to supplement operator in their role with adequate computer software[†] and new software for fault diagnosis and real time emergency procedure generation is under study (Varde et al., 1998; Varde et al., 1996; Kang et al., 1994; Chang et al., 1995). Nevertheless issues such as ergonomics and procedural adherence still rise (Daugherty, 1995).

[†] The newest Westinghouse AP600 design aims to having a computerized package of procedures to replace the step by step check list, but opposition has been encountered at a regulatory level.

4. Accident Mitigation

Mitigating Accident Management Procedures is the set of all actions intended to avoid containment failure and radiation release following core melt, making use of all the available equipment. Severe accident management is the term which groups all the studies and activities done in the area of post-core melt operations.

Severe accident management is the second phase in the management of an accident. Starting from a failure in the plant, the crew has been unable to avoid core uncovery, and now action must be taken to avoid containment failure and radioactivity release. We have underlined that, in the management of pre-core-melt upset plant conditions, EOPs are often linked to routine operational procedures, since at the start, an accident situation differs only slightly from normal operations. With severe accident management, this is no longer the case. Instrumentation will probably be lost and stress will be at the highest level for the operating crew. This problem has therefore been approached by restricting the number of severe accident management procedures to a few powerful ones which cover a broad spectrum of potentially severe plant states.

In severe accident management, phenomenological uncertainty plays a bigger role with respect to incident management. In fact, the prediction of the physical behavior of the core, after it has melted (the corium), is a difficult task: the density, displacement, temperature, chemical composition of the corium can be predicted only with great uncertainty. Furthermore hydrogen combustion and chemical reactions will be part of the already complex phenomenology.

The uncertainty about the events that characterize a post-core-melt accident introduces further issues related to model and completeness uncertainty. Model uncertainty means that we are not sure about the adequacy of the model we are using to describe the physical phenomena and essentially derives from the lack of experimental evidence. On the other hand, the task of predicting all the possible events and sequence bifurcation is almost impossible in terms of time and resources. Therefore, to achieve closure, methodologies must include a coherent treatment of model and completeness issues.

As mentioned previously, the purpose of severe accident management strategies is to avoid containment failure and radiation release. The effort is concentrated in the prevention of events such as vessel lower head failure, core concrete interaction, Zircaloy-water reactions (hydrogen combustion). After the Reactor Safety Study in the U.S., great effort was focused on the study of post core melt phenomena. Also, PRA was applied to individuate the failure modes of the containment. These studies started in the early 1980’s and continued to the present, although with some evolution.

In the following part of the report we will limit ourselves to two important severe accident management approaches both developed in the Unites States: the Risk Oriented Accident Analysis Methodology (Scobel et al, 1998; Theofanous et al., 1997; Tuomisto and Thoefanous, 1994) and the use of influence diagram for the analysis of an accident (Jae and Apostolakis, 1992; Jae et al., 1993; Milici et al., 1995; Catton and Kastenberg, 1998). As we will see, these two methodologies address different aspects of the accident management problem and will enable us to have a comprehensive view of the important issues in severe accident management and of potential approaches.

4.1 The Mark-I Containment Attack Problem: Example of a Severe Accident and Solution Approach.

In the late 1980s, PRA applied to containment failure modes identified the so called "Mark-I liner melt attack" problem in BWRs. Because of the tight MARK-I containment geometry, following lower head failure, the corium would spread in the containment sump (under the lower vessel head) and could reach the steel liner. (See Figures 11 and 12).

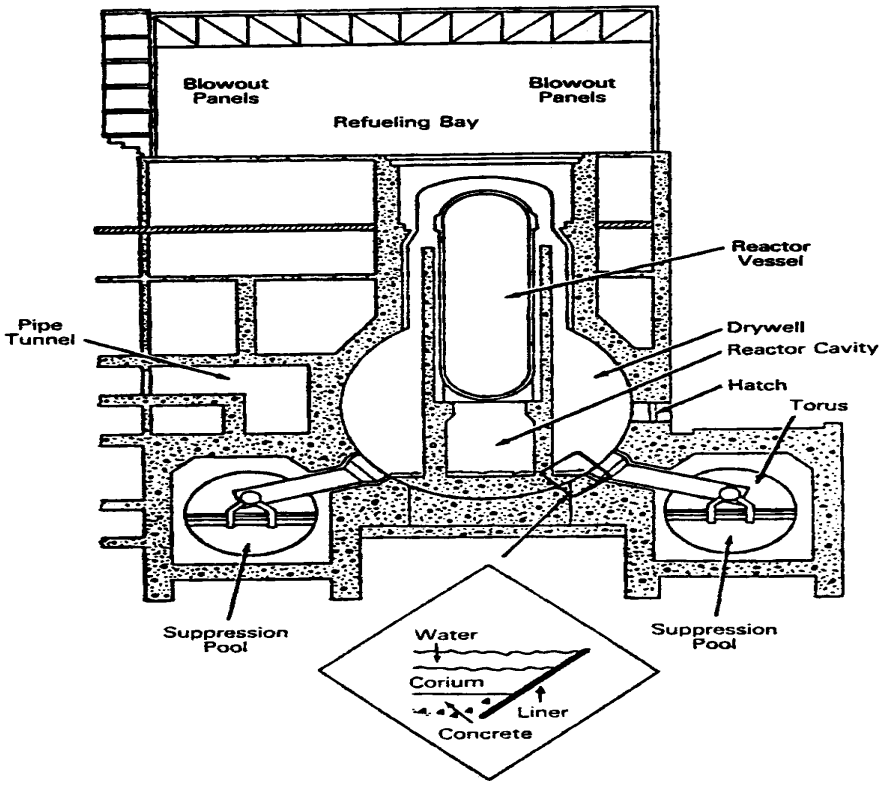


Figure 10. Mark-I containment.

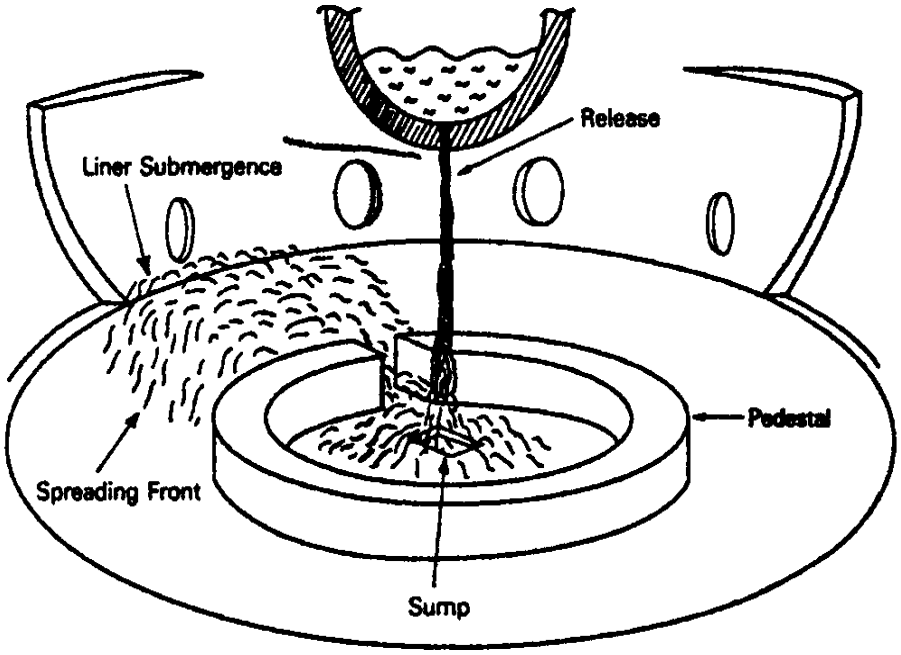


Figure 11. Corium falling in the containment sump from the lower head of the reactor vessel.

The high energetic content of the corium and its chemical activity would cause rapid corrosion and deterioration of the metallic containment shell therefore leading to containment failure. These issues were extensively debated and opposing opinions were given by experts and computer codes on the probability of liner failure. The problem of achieving closure was caused by the treatment of uncertainty; if not properly dealt with, uncertainties can pose serious doubts on the conclusion of a study. Closure was reached by applying the so called Risk Oriented Accident Analysis Methodology (ROAAM) for the analysis of the physical evolution of the accident. ROAAM proposes a decomposition of the problem into its deterministic and probabilistic aspects (see Figure 13) to create a probabilistic framework for the accident. This framework is characterized by the following elements:

S "Causal Relations": some physical phenomena can be described by well known physical laws (see for example Newton's law of cooling), and the pertaining parameters can be related through a deterministic model (called "Causal Relation"). In our case, for example, the height of the corium in the sump is deterministically related to the quantity of corium released.

S "Intangibles": some other phenomena are characterized by an intrinsic variability and they will be described by probability distributions. When required, expert judgment will be used to define the input distributions. In our case, the quantity of corium released will be described by a probability distribution.

S "Splinter Scenarios": given an initial plant damage state, the accident can evolve in different ways. Each scenario is one of the possible evolution mechanisms, and scenarios must be chosen so that they are independent. In the case of the Mark third liner attack, we start from the plant damage states containing lower head failure. Now, there are multiple ways in which the corium can be released into the containment sump. Three different ways were ultimately identified and used as different scenarios

1. Immediate release of a significant portion of the melt followed by a gradual release of the remaining quantity
2. A gradual release over an extended period
3. A large release of mainly solidified release (late lower head failure)

Suppose

$$L_i(H_k) = \mathcal{G}(p_1, p_2, \ldots p_\ell) \quad \textit{given} \quad D_i$$

where $\{D_i\}$ is a set plant damage states satisfying

$$f_s < f_i(D_i) < f_t$$

Decompose into framework and scenarios, $\{S_{ij}\}$, such that

$$L_i(H_k) < L_{ij}(H_k)$$

where

$$L_{ij}(H_k) = \mathcal{F}(d_1, d_2, \ldots i_1, i_2, \ldots)$$

and

$\{i_i\}$ is a set of "intangible" parameters

$\{d_i\}$ is a set of "deterministic" parameters

Quantify $L_{ij}(H_k)$ based on probability scale, to show that

$$P_{ij}(H_k) < P_s \quad \textit{given} \quad \{D_i\} \quad \textit{for all} \quad \{S_{ij}\}$$

where P_s is the "physically unreasonable" level.

The probability scale is arbitrary.

Figure 12. The steps of the ROAAM process.

Once this probabilistic framework has been created, the probability of hazard j, (H_j), will be calculated, given the set of all the initial plant damage states and the set of all the scenarios associated with the damage state $D_{i...}$. In our example, hazard j would be containment failure, and the damage states would be the set of plant damage states with lower head vessel failure (they would obviously depend on the PRA definition).

The main scope of ROAAM is to provide adequate identification and treatment of uncertainties, separating epistemic and aleatory uncertainties. The completeness issue is resolved considering the plant damage states with a frequency between a certain upper value f_t (threshold frequency) and a lower value f_s (screening frequency). The value f_t is established by the prevention goals (for example, the frequency of a certain plant damage state cannot be higher than the core damage frequency). The value f_s is a screening frequency below which events can be regarded as physically unreasonable. In other words, we know that our model will not be exhaustive, but we have enveloped the most important aspects.

ROAAM has been applied to the study of the physical effectiveness of severe accident management strategies, such as the in-vessel retention strategy for the Loviisa NPP in Finland and the new Westinghouse AP600 showing that the probability of H_j is lower than a certain established value.

The effectiveness of a strategy is measured on the basis of appropriately defined safety goals. In the case of AP600, the ROAAM has been used to demonstrate that the passive systems assure a containment failure probability of less than one tenth given a core damage event.

4.2 A General Framework for Severe Accident Management Strategies Evaluation

Five criteria have been identified by the U.S. Nuclear Regulatory Commission for the assessment of a severe accident management strategies:

1. The feasibility of the strategy
2. The effectiveness of the strategy
3. The possibility of adverse effects
4. Information needs
5. Compatibility with existing rules and procedures.

The first criterion is related to the probability that the strategy will be correctly implemented once the plant operators are instructed to take the relative actions. The effectiveness of a

severe accident management strategy is related to its technical characteristics (for example the amount of water to be released in the cavity to assure adequate core cooling). Effectiveness assessment of severe accident management is a complicated problem because of the complex phenomena involved in a severe accident and the large uncertainty about the physical models and the associated parameters[†].

The possibility of adverse effects deals with the fact that the implementation of the procedures must not impair existing equipment (in effect, worsening the plant conditions) and must not change the course of the accident towards an undesirable directions. For example, an inappropriate timing of dumping water could cause a steam explosions that may threaten containment integrity.

Information needs refer to the quantity of information necessary to implement the strategy, considering that, in a severe accident, much of the instrumentation will be damaged. Also, issues such as the delay in dealing with current plant status information is considered.

Finally the compatibility issue consider the impact of the strategy on existing procedures and rules. This issue is a regulatory concern, but it is important in that a regulatory framework surrounds the operation of all nuclear power plants.

These five criteria state clearly that engineering analysis of a strategy, although accompanied by PRA insights, is not sufficient to its evaluation. In section 3 we have discussed how the complete definition of the problem should be thought of as a sequential decision making in presence of uncertainty. Decision theory is the discipline that deals with the problem of decision making under uncertainty, and influence diagrams are powerful tools for the representation and solution of decisional problems. We will now describe the general features of the application of these methodologies to severe accident management (Jae and Apostolakis, 1992; Jae et al., 1993; Milici et al., 1995; Catton and Kastenberg, 1998).

[†] Experiments have been performed to reduce the uncertainty on the physics of a severe accident, and, in particular, to confirm the feasibility of the in-vessel-retention strategy. We recall here the COPO and mini-ACOPO experiments at UCLA (USA).

Let us suppose that at a certain plant[†] following a short-term station-blackout accident the operating staff is left with the following alternatives:

1. Cavity flooding
2. Primary system depressurization
3. Feed and bleed if alternating current (AC) power is recovered before vessel failure.

In theory, the first two procedures can be implemented concurrently while the third procedure needs the recovery of AC power. But, alternative three is definitely implemented in case the first two procedures are not successful. The influence diagram representing this situation is plotted in Figure 14

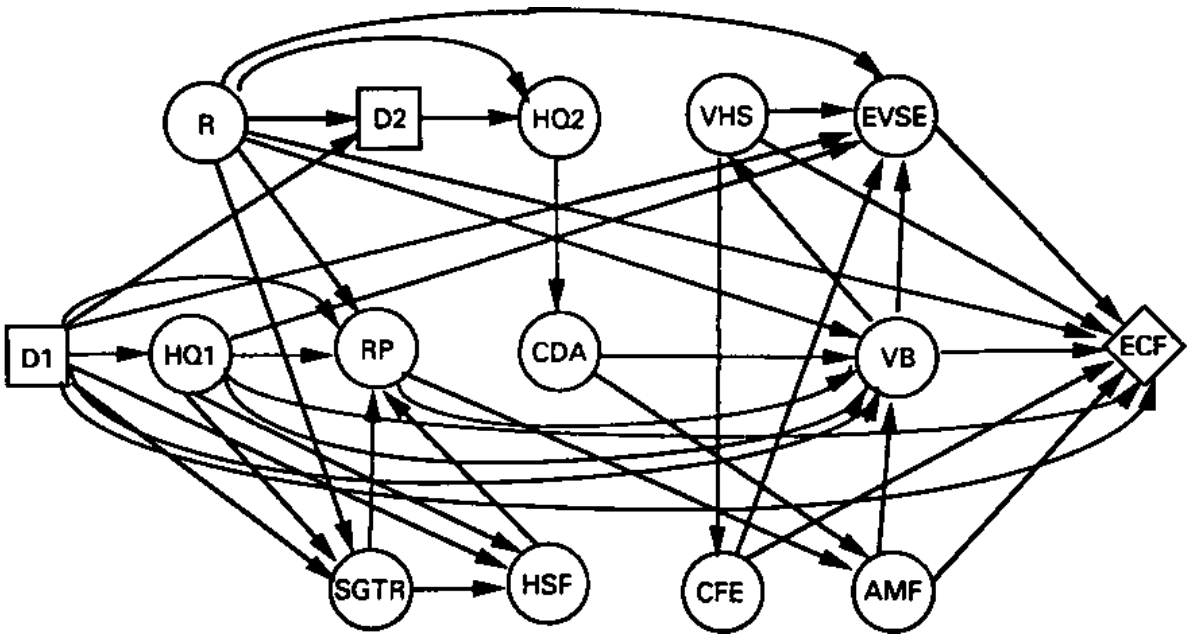


Figure 13. Influence diagram for evaluation of accident management strategies at Surry, U.S.

Two decision nodes are present, indicating the sequential nature of the decision problem associated with accident management. The circles represent events (chance nodes) whose occurrence is "random" in the sense that they are not under the complete control of the decision maker. The two rectangles represent the two decisions: the first node (D1) will have three outcomes: flooding only, depressurizing only, or both. The second node represents the decision to feed and bleed and it has two possible options: feed and bleed or do nothing. Arcs that go into

[†] The study Jae et al., 1993 was done for the NPP at Surry Virginia, USA.

a decision node represent the information available to the decision maker at the moment of the decision. For example, node "R" represents the event "recovery of AC power" and we know that such information is necessary to the decision maker to implement feed and bleed.

A great advantage of influence diagrams is that they enable the analyst to represent in a compact way the complex dependencies of the problem. For example, the recovery of AC power (node R) will influence not only the decision maker state of information, but also will influence the probability of steam generator tube rupture (SGTR) and the pressure in the reactor coolant system (Jae et al., 1993). Connecting arcs will be drawn from node "R" to the corresponding nodes.

Particular attention is deserved for nodes HQ1 and HQ2, which represent the event "the staff successful implementation of the required procedures." They represent probabilistic events and the determination of their probability requires the use of human reliability analysis techniques. The main consideration here is that influence diagrams allow a simple integration of the man-machine-interface analysis.

Finally, the strategy will be evaluated against a certain "Value" or "Utility" established by the decision maker . In general, the "Value" can range from Core Damage Frequency (Events per Year) to Large Early Release Frequency (Events per Year) to Costs or Productivity ($), depending on the decision maker. In our example, the conditional frequency of Early Containment Failure [P(ECF)] is the evaluation criterion. The best strategy will assumed to be the one which allow the lowest P(ECF) on an Expected Value (EV) basis (see Table 2). However, since we are dealing with uncertain quantities, this result would not be complete if we do not add information about how much we are uncertain about the result.

Influence diagrams enable sensitivity analysis and uncertainty propagation in a direct way. Sensitivity analysis shows the effects of changes in the input parameters on the output predictions. It is then possible to evaluate which parameters have the greatest impact on the "Value." It is logical to expect that uncertainties on these parameters will be the main contributors to the global uncertainty. Propagation of the uncertainty on the input parameters to the output through the influence diagram and will tell us how uncertain we are on estimates of the "Value."

In our example, we had eight combinations due to the three possible decision in the first node and two decisions in the second node (Table 2). Based on the expected value of the ECF, the best strategy would be to depressurize only and than to go to feed and bleed in case of AC power recovery. The ranking of the eight alternatives is sensitive to the value of several variables, most of which are directly related to phenomenological issues about which there is a

considerable amount of uncertainty. Changes in the state of knowledge on these parameters could change the final ranking of the alternatives.

Table 2. Example of decision alternatives ranking obtained applying influence diagrams to severe accident management strategies (Jae et al., 1993).

Decision Alternative	Rank	P(ECF)
Flood only/Feed and Bleed	2	6.34E-3
Flood only/Do Nothing	6	1.15E-2
Depressurize only/Feed and Bleed	1	5.25E-3
Depressurize only/ Do Nothing	5	1.04E-2
Flood and Depressurize/ Feed and Bleed	4	7.14E-3
Flood and Depressurize/ Do Nothing	8	1.23E-2
Do Nothing/ Feed and Bleed	3	6.89E-3
Do Nothing/ Do Nothing	7	1.20E-2

Notes for Table 2: Mean Values and Ranking for the decision alternatives of our example (Jae et al., 1993). The twofold action connected with each alternative (ex. Flood only/Feed and Bleed) derives from the sequential nature of the decision. Once an initial strategy has been chosen, there is the possibility to do nothing or to go to feed and bleed. P(ECF) is the conditional probability of early containment failure, and it is assumed as evaluating parameter. The alternatives will be ranked from the one with the lowest P(ECF) value to the one with the highest P(ECF).

5. Conclusions

One of the main conclusions of our review is that accident management is undoubtedly an area of major interest to the international nuclear community. As it can be seen in the bibliography (Appendix A), many of the countries with a nuclear power program have research ongoing in the area of incident management or severe accident management. A great variety of methodologies have been developed to cope with the several aspects (e.g., timing, uncertainties, decision making, phenomena) of accident management, thus signalizing how complex and vast the subject is.

Another important insight is that uncertainties play a major role in assessing the validity of accident management strategies and must be appropriately taken into account. This treatment of uncertainties both determines how certain analysis methods are formulated (and subsequently performed) and how final results are utilized and presented.

PSA methods are the basis of the analysis of incident management or severe accident management strategies even though static PSA and other simple technical engineering analyses are not sufficient to deal with all the aspects of the problem. Dynamic event trees have attempted to replaced static event trees in the evaluation of the efficacy of emergency operating procedures. Software packages based on discrete dynamic event trees have been developed to assist operators in their tasks during both normal and upset plant conditions. In addition, research has taken place in the pursuit of "forcing" static-type of PSA models to better represent dynamic situations.

We have seen that the technical effectiveness of a strategy is only one of the requirements of the ideal set of procedures.

The characteristics of the ideal procedure can be summarized as follows:

- Feasibility of the strategy
- Effectiveness of the strategy
- Absence of adverse effects: the procedure may not unacceptably interfere with plant design
- Information needs
- Compatibility with existing rules and procedures
- Operator grace time
- Possibility of interruption and resumption

The evaluation of a strategy based only on its technical requirements (effectiveness) is therefore not exhaustive. The problem must be considered as a decision-making problem with sequential decisions under uncertainty. Influence diagrams have revealed themselves as the appropriate tools to perform such an analysis, allowing:

- Compact and clear representation of the complex dependencies among the parameters of the problem

- Adequate and direct individuation and propagation of the uncertainties.

Two distinguished working areas can be identified: the pre-core-damage area (prevention) and the post-core-damage area (mitigation). In the context of traditional "accident management" research and development, the focus has been on mitigation. This focus has resulted in the utilization of the Level 2 PSA as a primary tool for determination of the accident sequence context.

Prevention is characterized by the use of EOPs, which departs from the routine operations. In this case, the role of the decision maker is the shift supervisor and the actions are taken in order to restore normal plant operations.

Mitigation is characterized by the use of accident management procedures that normally differ considerably from the EOPs. The role of the decision maker in this case could not be so well defined as in the previous case and depends strongly on the organization. And, as is well known, the operation of a particular organization depends on the country and on the facility. In the case of a severe accident, the facility is required (e.g., U.S., France, Sweden) to alert the public authorities. Emergency organization will gather in a strategic center(s) (e.g., Paris, Washington D.C.) and experts will communicate within and outside the border of the plant and the control room. In this case, the role of the decision maker is not clear. Furthermore, if the accident spans a significant length of time, different persons may have to deal with the same decision. Therefore, the roles of the decision maker and of the organization are open issues in the formulation of accident management strategies.

Another issue is related to the interpretation of the EOPs. In the U.S., the EOPs are intended to be followed step-by-step. A different attitude is encountered in other countries such as France where the EOPs are seen more as guidelines to operation. This raises the question of which of the two attitudes is the most effective in an accident management strategy.

6. References

Apostolakis, G. E., 1995. "A Commentary on Model Uncertainty," in: *Proceedings of Workshop on Model Uncertainty,"* A Mosleh, N. Siu, C. Smidts, and C. Lui, Eds., Center for Reliability Engineering, University of Maryland, College Park, MD (also published as Report NUREG/CP-0138, US Nuclear Regulatory Commission, Washington, DC, 1994).

Catton, I., and W.E. Kastenberg: "Reactor Cavity Flooding as an Accident Management Strategy," *Reliability Engineering and System Safety*, 62:59-70, 1998.

Chang H.S., K. S. Kang, and S. H. Chang, "Development of Severe Accident Management Support System Using Quantified Containment Event Trees," *Reliability Engineering and System Safety*, 48, 205-216, 1995.

Dougherty, E. M., "Credibility and uncertainty associated with accident management actions," *Reliability Engineering and System Safety*, 37, 1992, 45-55.

Daugherty, E., "EOPs, A Lingering Concern," Letter to the editors, *Reliability Engineering and System Safety*, 48, (1995), 235-238, 1995.

Götz, W., *Influence Diagrams and Decision Trees for Severe Accident Management*, Netherlands Energy Research Foundation, ECN-R—96-004, September 1996.

Hsueh, K. S., A. Mosleh,: " The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants", *Reliability Engineering and System Safety*, 52, 297-314, 1996

Jae, M., G. Apostolakis, "The Use of Influence Diagrams for Evaluating Severe Accident Management Strategies," *Nuclear Technology*, 99:142-157, 1992.

Jae, M., A. Milici, W. Kastenberg, and G. Apostolakis, "Sensitivity and Uncertainty Analysis of Accident Management Strategies involving Multiple Decisions," *Nuclear Technology*, 104: 13-36, 1993.

Kang, K.S., H. S. Chang, and S. H. Chang, "Development of Advanced Procedure for Emergency Operation Using Task Allocation Synthesis and PRA Results," *Reliability Engineering and System Safety*, 45, 249-259, 1994.

Milici, A., J.-S. Wu, G. Apostolakis, K-F. Yau: *Accident Management Advisor System Development to handle Uncertain Sensor Inputs under Nuclear Plant Accident conditions*, prepared for U.S. Department of Energy, Phase II Report, 1995.

Roth-Seefrid, H., A. Feigel, H.-J. Moser: "Implementation of Bleed and Feed Procedures in Siemens PWRs," *Nuclear Engineering and Design*, (1994), 148, 133-150.

Sanchez, M., J.Melara: "Extending PSA to Accident Management: the Case of the Steam Generator Tube Rupture (STGR). Emergency Operating Procedures Assessment", *Proceeding of the International Conference On Nuclear Engineering (ICONE)*, Volume 3, ASME, 1996

Schouten, H., *A Fault Tree Based Real Time Operator Support System*, (URL: http://www-mr.wbmt.tudelft.nl/mms/supervis/schouten), Netherlands Energy Research Foundation, July 1998.

Scobel, J. H., T. G. Theofanus, S. W. Sorrell, "Application of the Risk Oriented Accident Analysis Methodology (ROAAM) to Severe Accident Management in the AP600 Advanced Water Reactor," *Reliability Engineering and System Safety*, 62,1-2 Oct., Nov., 1998

Svenson, O., "A Decision Theoretic Approach to an Accident Sequence: When Feedwater and Auxiliary Feedwater Fail in a Nuclear Power Plant," *Reliability Engineering and System Safety*, 59, 243-252, 1998.

Swain, A. D., H.E. Guttman, *Handbook of Human Reliability Analysis with an Emphasis on Nuclear Power Plant Application*, NUREG/CR-1278, Nuclear Regulatory Commission, Washington, 1983.

Theofanous, T. G., C. Liu, S. Additon, S. Angelini, O. Kymalainen, T. Salmassi, "In-vessel Coolability and Retention of a Core Melt", *Nuclear Engineering and Design*, 169, (1997),1-48.

Tuomisto, H., T. G. Thoefanous: "A Consistent Approach to Severe Accident Management," *Nuclear Engineering and Design*, 148, 171-183, 1994.

Varde,, P. V., S. Sankar, A. K. Verma, and P. Praskash, "OPAD–An Expert System for Research Reactor Operations and Fault Diagnosis," *Proceedings of ASME/JSME's Fourth International Conference on Nuclear Engineering, (ICONE-4),* 1996.

Varde, P. V., S. Sankar, and A. K. Verma, "An Operator Support System for Research Reactor Operations and Fault Diagnosis Through a Connectionist Framework and PSA Based Knowledge Bases Systems," *Reliability Engineering and System Safety*, 60, 53-69, 1998.

Appendix A – Bibliography

Belgium

V. Lhoest, R. Bastien, *A Successful Approach for the Implementation of Symptom-Based Emergency Operating Procedures for VVER Reactors*, ICONE5-2581, May 1997.

> This paper looked at the VVER emergency operating procedures as a method of providing preventative measures against the onset of core damage. While the procedures would be symptom-based, they are nonetheless prescriptive and do not formally incorporate decision making into the accident as it is developing.

France

Y. Cornille, "Accident Management for French PWRs," *Nuclear Engineering and Design*, 148 (1994) 161-170.

> The accident management scheme as it exists now for French pressurized water reactors has been developed in stages over a period of more than 10 years. The requirement - equipment, procedures, structures, communication and transmission systems - are operational although (at the moment the paper was written) improvements are still to be considered. Throughout this development, the goal has been to increase the protection of the public by improving and extending the defense in depth. This extension has been done pragmatically, looking for further protection against credible events so as to result in a coherent construction. Should an accident occur, the management scheme would allow the plant operator Electricite de France and the government authorities to exercise fully their responsibilities. The paper first describes the stages in the development of the severe accident management scheme and the rationale behind it, then the measures developed to prevent or mitigate the consequences of a severe accident including the technical bases and, finally, the emergency organization for the case of a severe accident at a pressurized water reactor.

Finland

H. Tuomisto, T. G. Thoefanous: "A Consistent Approach to Severe Accident Management," *Nuclear Engineering and Design*, 148, 171-183, 1994.

> This paper aims at describing the severe accident management approach developed at the Loviisa NPP in Finland. The main goal of the approach is the study of a strategy to assure a containment failure of less than 10-2. The envisioned strategy is based on the concept of in-vessel retention of the core melt. As a result some hardware changes in the plant have to be made to increase the possibility of success of the strategy. These changes allow lowering of the lower head thermal

insulation and neutron shield assembly, opening of the doors of the ice condenser and spraying the external steel shell of the containment. It is expected that in vessel coolability will be feasible if these changes are implemented: in fact, gradual hydrogen combustion and long term stabilization of the containment pressure should be achieved.

Germany

T. Mull, M. Perst, K. Umminger, *Effectiveness of Accident Management Procedures under Small Break LOCA Conditions – Experimental Results from the PKL-Test Facility*, ICONE5-2194, May 1997.

The paper discussed tests that were preformed for small-break LOCA scenarios and comparisons of existing accident management procedures and as-built safety margins. Insights gained from the tests indicted that operator management procedures would be successful. In addition, they tied the analysis back to other analysis looking at secondary side depressurization and subsequent "feed and bleed."

H. Roth-Seefrid, A. Feigel, H.-J. Moser: "Implementation of Bleed and Feed Procedures in Siemens PWRs," *Nuclear Engineering and Design*, (1994), 148, 133-150.

This paper describes in a detailed way the work done in Germany to implement Feed and Bleed strategy to prevent core melt in Siemens BWRs. Analysis of the Emergency operating is based on PRA insights, and the overall conclusion is that the adoption of this strategy will reduce core damage frequency by at least a factor four.

Hungary

G. Ezsol, L. Perneczky, and L. Szabados, *An Experimental and Analytical Study in Support of the Development of Accident Management Procedures for VVER Reactors*, ICONE5-2463, May 1997.

The concept of accident management beyond design basis was not implemented in the VVER-type plants at the time of publication of this paper. Consequently, the authors performed typical thermohydraulic calculations to support the development of prescriptive, static accident management plans.

India

Varde, P. V., S. Sankar, and A. K. Verma, "An Operator Support System for Research Reactor Operations and Fault Diagnosis Through a Connectionist Framework and PSA Based Knowledge Bases Systems," *Reliability Engineering and System Safety*, 60, 53-69, 1998.

> It is well known that during reactor upset/abnormal conditions, emphasis is placed on the plant operator's ability to quickly identify the problem and perform diagnosis and initiate recovery action to ensure the safety of the plant. The availability of operational aids capable of monitoring the status of the plant and quickly identifying the deviation from normal operation is expected to significantly improve the operator reliability. This paper describes the development of an operator support systems based on probabilistic safety assessment (PSA) techniques. An efficient approach using artificial neural networks for safety status/transient condition monitoring and rule-based systems for diagnosis and emergency procedure generation has been applied for the development of a prototype operator adviser (OPAD) system for a 100 MW(th) heavy water moderated, cooled and natural uranium fueled research reactor. The development objective of this system is to improve the reliability of operator action and hence the reactor safety at the time of crisis as well as in normal operation. Conclusions of the testing are that it can efficiently identify the reactor status in real-time scenario.

P. V. Varde, S. Sankar, A. K. Verma, and P. Praskash, "OPAD–An Expert System for Research Reactor Operations and Fault Diagnosis," *Proceedings of ASME/JSME's Fourth International Conference on Nuclear Engineering, (ICONE-4),* 1996.

> This paper describes the development of a prototype Knowledge Based (KB) operator Adviser (OPAD) system for 100 MW(th) Heavy Water moderated, cooled and Natural Uranium fueled research reactor. The development objective of this system is to improve the reliability of operator action and hence the reactor safety at the time of crises as well as normal operation.

Korea

Kang, K.S., H. S. Chang, and S. H. Chang, "Development of Advanced Procedure for Emergency Operation Using Task Allocation Synthesis and PRA Results," *Reliability Engineering and System Safety*, 45, 249-259, 1994.

> This paper describes an advanced emergency operating procedure (AEOP) for emergency operation. Attention is focused on the importance of the operator's role in emergency conditions for nuclear power plants (NPPs). To overcome the complexity of emergency operating procedures (EOPs) and maintain the consistency of action steps according to plant emergency conditions, operator tasks are allocated according to their duties in the AEOP and a computerized operator aided system (COAS) is developed as an alternative to reduce the operator's burden and provide the detail action procedures. The PRA (Probabilistic Risk Assessment) results are synthesized in the AEOP using the event tree (ET) to give awareness and prediction of accident progression in advance. The time response for completing the required action is observed to

evaluate the impact of the AEOP with COAS on operator performance during the loss of offsite power (LOOP) scenario with the full scope simulator of NPP at Kori. The results indicated that operator actions using AEOP are not only more consistent but are also able to provide earlier termination and mitigation of accidents.

Chang H.S., K. S. Kang, and S. H. Chang, "Development of Severe Accident Management Support System Using Quantified Containment Event Trees," *Reliability Engineering and System Safety*, 48, 205-216, 1995.

The Probabilistic Risk Assessment (PRA) for a nuclear power plant can provide so much valuable information including plant-specific vulnerabilities against severe accident, which is quite useful in developing severe accident management strategies. In this study, the information regarding Containment Event Trees obtained by performing PRA is introduced to develop the suitable event-oriented severe accident management strategies. For these, it is crucial to identify the exact state of severe accident progression which is called Plant Damage State as an entrance condition. However, there are several areas where insufficient knowledge exists at the moment and thus it can be impossible to identify the event correctly. In this study, symptom-oriented strategies are also provided as an alternative methodology by using safety objective tree method to circumvent such drawback. Both event-oriented and symptom-oriented approaches are synthesized into a computerized supporting system for severe accident management, and linked with a severe accident simulator for on-line verification. A sample sequence is selected to show the simulated results performed by the system. Simulation results show that this kind of methodology might be quite useful in developing and implementing severe accident management strategies.

S. H. Ghyym, "Overview of In-vessel Retention Concept Involving Level of Passivity: with Application to Evolutionary PWR Design", *Annals of Nuclear Energy*, **25**,13, September 1998.

In this work, one strategy of severe accident management, the applicability of the in-vessel retention (IVR) concept, which has been incorporated in passive type reactor designs, to evolutionary type reactor designs, is examined with emphasis on the method of external reactor vessel cooling (ERVC) to realize the IVR concept in view of two aspects: for the regulatory aspect, it is addressed in the context of the resolution of the issue of corium coolability; for the technical one, the reliance on and the effectiveness of the IVR concept are mentioned. Additionally, for the ERVC method to be better applied to designs of the evolutionary type reactor, the conditions to be met are pointed out in view of the technical aspect. Concerning the issue of corium coolability/quenchability, based on results of the review, plausible alternative strategies are proposed. According to the decision maker's risk behavior, these would help materialize the conceptual design for evolutionary type reactors, especially Korea Next Generation Reactors (KNGRs), which have been developing at the Korea Electric Power Research Institute (KEPRI): (A1) Strategy 1A: strategy based on the global approach using the reliance on the wet cavity method; (A2) Strategy 1B: strategy based on the combined approach using both the reliance on the wet cavity method and the counter-measures for preserving

containment integrity; (A3) Strategy 2A: strategy based on the global approach to the reliance on the ERVC method; (A4) Strategy 2B: strategy based on the balanced approach using both the reliance on the ERVC method and the countermeasures for preserving containment integrity. Finally, in application to an advanced pressurized water reactor (PWR) design, several recommendations are made in focusing on both monitoring the status of approaches and preparing countermeasures in regard to the regulatory and the technical aspects.

The Netherlands

W. Götz, *Influence Diagrams and Decision Trees for Severe Accident Management*, Netherlands Energy Research Foundation, ECN-R—96-004, September 1996.

This report provided a review of formal decison methods (influence diagrams, decision trees, event trees) in the context of traditional severe accident analysis methods. As part of the work, a Level 2 case study was utilized. The study demonstrated that influence diagrams and decision trees have advantages over just using risk assessment event trees for severe accident management.

H. Schouten, *A Fault Tree Based Real Time Operator Support System*, (URL: http://www-mr.wbmt.tudelft.nl/mms/supervis/schouten), Netherlands Energy Research Foundation, July 1998.

This work provides a general outline into the development of an operator aid (for decision making) based upon a combination of timing considerations and traditional fault tree logic models. Special “time nodes” are introduced into the fault tree logic in order to obtain timing information related to failures of complex systems. This timing information is then relayed to the operators (along with failure information) to improve the decision process.

Spain

CSN MARS Development, Fauske & Associates

Consejo de Seguridad Nuclear (CSN), headquartered in Madrid, Spain, is the Spanish nuclear regulatory agency. CSN is responsible or monitoring the accident and advising the other Spanish governmental institutions, consistent with the Spanish Emergency Plan, during an accident situation at a Spanish plant. To assist CSN during an emergency, CSN selected Fauske & Associates, Inc. to develop and maintain an on-line accident management software system called MARS (MAAP Accident Response System).

M.Sanchez, J.Melara: "Extending PSA to Accident Management: the Case of the Steam Generator Tube Rupture (STGR). Emergency Operating Procedures Assessment", *Proceeding of the International Conference On Nuclear Engineering (ICONE)*, Volume 3, ASME, 1996

> This paper presents the conceptual basis of the DYLAM-TRETA-HOI code, (see the report) for the evaluation of the efficacy of EOPs. The methodology is based on the use of Discrete Dynamic Event Trees to describe the temporal evolution of the plant as the actions required in the procedures take place. Changes in the procedures or need for links to other procedures are underlined in the case of Steam generator tube rupture.

Sweden

G. Lowenhielm, A. Engquist, R. Espefalt, "Accident Management Strategy in Sweden-Implementation and Verification," *Nuclear Engineering and Design*, 148 (1994), 151-159

> This paper describes the program for severe accident management completed in Sweden by the end of 1988. This program included plant modifications such as the introduction of filtered containment venting and an accident management system comprising emergency operating strategies and procedures, training and emergency drills.

O. Svenson, "A Decision Theoretic Approach to an Accident Sequence: When Feedwater and Auxiliary Feedwater Fail in a Nuclear Power Plant," *Reliability Engineering and System Safety*, 59, 243-252, 1998.

> Ola Svenson is currently professor in the department of psychology at the university of Stockholm. In this paper he deals with the problem of accident management from a decision theoretic perspective. Indications on human reliability models and important consideration on the human-machine interface are given.

Swiss

Dr. Serge Prêtre, *Keynote Address -- Decision-making in Abnormal Radiological Situations*, Swiss Nuclear Safety Inspectorate (HSK), Villigen-HSK, Switzerland

> This paper covers the keynote address (outlining several ideas) for the CRPPH - Working Group on Societal Aspects. These ideas that are presented emerged mainly after it became evident that the post-Chernobyl contamination has caused an enormous societal problem. The workshop addresses other examples in addition to Chernobyl. The keynote address consisted of 18 flip-charts in addition to the speech.

Planning and Execution of Emergency Exercises in Swiss Nuclear Power Plants, Swiss Federal Nuclear Safety Inspectorate, Section for Nuclear Technology and Safety (NS), February 1998.

> The objective of this report was to provide an overview of the guidelines produced by the Swiss Nuclear Safety Authority and list how this organization intends to fulfill its statutory responsibilities. The guidelines indicate how nuclear plant operators will comply in their application and evaluation of tasks related to surveillance of accident management tests. The present guideline is designed to regulate the planning and conduct of emergency safety exercises at Swiss nuclear power plants.

Responsibility for Decisions to Implement Certain Measures to Mitigate the Consequence of A Severe Accident at a Nuclear Power Plant, Swiss Federal Nuclear Safety Inspectorate, Guideline HSK-R-42.

> This guideline provides a brief overview of expectation from the regulator to plant operators concerning their responsibility to mitigate a severe accident.

United States

U.S. Nuclear Regulatory Commission, Severe Accident Management Demonstrations, 1998

> The NRC has attended and critiqued several accident management demonstration implementations at U.S. nuclear power plants. The motivation for the plant visits was to observe how accident management plans were being implemented. While U.S. accident management activities have focused exclusively on the Level 2 and Level 3 part of a severe accident, several insights are worth mentioning: Several severe accident management tools are also used for events that do not lead to core damage (e.g., trending charts, guidelines for core assessment); some potential management strategies were not implemented since they may lead to unreviewed safety questions; limitations in the drill (practice) scope could lead to artificial decision making; information exchange between plant organizations was less than optimal; and the plant operators had difficulties diagnosing the accident situation and tracking plant parameters.

M. Jae, G. Apostolakis, "The Use of Influence Diagrams for Evaluating Severe Accident Management Strategies," *Nuclear Technology*, 99:142-157, 1992.

> This papers demonstrates the use of influence diagrams for the evaluation of severe accident management strategies. Fundamentals of this technique are presented with application to a case study.

M. Jae, A. Milici, W. Kastenberg, and G. Apostolakis, "Sensitivity and Uncertainty Analysis of

Accident Management Strategies involving Multiple Decisions," *Nuclear Technology*, 104: 13-36, 1993.

> In this paper, a comprehensive evaluation of accident management strategies based on influence diagrams is presented. The case study is the short-term station blackout sequence for the Surry NPP in Virginia, USA. Three strategies are evaluated: cavity flooding, depressurization and feed and bleed. The strategies are at first evaluated based on the expected value of the conditional frequency of Early Containment Failure. Sensitivity analysis and uncertainty propagation are then performed to individuate the changes in the ranking of the alternatives due to uncertainties.

A. Milici, J.-S. Wu, G. Apostolakis, K-F. Yau: *Accident Management Advisor System Development to handle Uncertain Sensor Inputs under Nuclear Plant Accident conditions*, prepared for U.S. Department of Energy, Phase II Report, 1995.

> This report, written for the U.S. Department of Energy, describes the design, development and demonstration of functionality of the Accident Management Advisor System (AMAS) software. The software is intended to support the functions of technical personnel and operators during an accident or abnormal conditions at a nuclear power plant.

I. Catton and W.E. Kastenberg: "Reactor Cavity Flooding as an Accident Management Strategy", *Reliability Engineering and System Safety*, 62:59-70, 1998.

> Reactor cavity flooding is a severe accident management that aims at avoiding lower head failure. In this paper the impact of uncertainty of deterministic models parameters important in the flooding of the cavity is evaluated. Influence diagrams are the tools utilized to perform the analysis. Early (EF) and Late (LF) fatalities are the two attributes for the strategy evaluation. Conclusions are that based on EF to flood the cavity is the best option, while in terms of LF doing nothing would be the best strategy. If the cavity is flooded there will be no lower head failure. But, a definitive conclusion about this accident management strategy cannot be reached due to phenomenological uncertainty.

K. S. Hsueh, A. Mosleh,: " The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants", *Reliability Engineering and System Safety*, 52, 297-314, 1996

> This paper describes the principal modeling concepts, practical aspects, and an application of the Accident Dynamic Simulator (ADS) developed for full scale dynamic probabilistic risk assessment (DPRA) of nuclear power plants. Full scale refers not only to the size of the models, but also to the number of potential sequences which should be studied. Plant thermal-hydraulics behavior, safety systems response, and operator interactions are explicitly accounted for as integrated active parts in the development of accident scenarios. ADS uses discrete dynamic

event trees (D-DET) as the main accident scenario modeling approach, and introduces computational techniques to minimize the computer memory requirement and expedite the simulation. An operator model (including procedure-based behavior and several types of omission and commission errors) and a thermal-hydraulic model with a PC run time more than 300 times faster than real accident time are among the main modules of ADS. To demonstrate the capabilities of ADS, a dynamic PRA of the Steam Generator Tube Rupture event of a US nuclear power plant is analyzed.

J. H. Scobel, T. G. Theofanus, S. W. Sorrell, "Application of the Risk Oriented Accident Analysis Methodology (ROAAM) to Severe Accident Management in the AP600 Advanced Water Reactor," *Reliability Engineering and System Safety,* 62,1-2 Oct., Nov., 1998

An important part of the AP600 design, as well as of the design certification review by the US Nuclear Regulatory Commission, is devoted to ensuring defense in depth through deep consideration and management of severe accidents. This paper shows the application of the Integrated ROAAM to the study of the passive safety features of the AP600, and demonstrates that containment bypass and containment isolation failure are remote and speculative.

T. G. Theofanous, C. Liu, S. Additon, S. Angelini, O. Kymalainen, T. Salmassi, "In-vessel Coolability and Retention of a Core Melt", *Nuclear Engineering and Design*, 169, (1997),1-48.

Based on the risk oriented accident analysis methodology, the efficacy of external flooding of a reactor vessel as a severe accident management strategy is assessed for an AP600-like reactor design. Including bounding scenarios and sensitivity studies and parametric evaluations that allow for the delineation of failure boundaries, the assessment demonstrates that the lower head failure is physically unreasonable. Use of this conclusion for any specific application is subject to verifying the required reliability of the depressurization and cavity-flooding systems, and to showing the appropriateness of the thermal insulation design and of the external surface properties of the lower head.

E. Borgonovo, R. Weil, and C. Smith, *Nuclear Power Plant Event Management Using A Formal Decision-Making Process*, Massachusetts Institute of Technology, 15.065 Class Project, March, 1999

Since a nuclear power plant (NPP) is a complex, technological system, a variety of events or occurrences could happen during the normal course of operation. These events span the gamut from simple, non-safety-related component outages to complex plant transients that may lead to damage of the reactor core. But, one attribute that all of these events currently have in common is that the plant operators/owners respond to the event using a purely "engineering" decision mechanism. In other words, formal decision analysis techniques are not typically used during the operation of today's NPPs. The report presents a formal decision analysis methodology that is

applicable to the treatment of both emergency and non-emergency type events. In addition, a generic representation of the methodology is formulated to provide a high-level view of the overall framework. Using this framework, they discuss and analyze three typical events that could occur during operation of a NPP, a failure of a main feedwater train, a failure of a diesel generator, and a failure of a reactor core fuel pin.

S. A. Hodge and M. Petek, "Assessment of Two BWR Accident Management Strategies," *Nuclear Engineering and Design*, 148 (1994), 185-203.

After TMI work has been done in the USA national laboratories to study the feasibility and efficacy of accident management strategies from a technical point of view. In this paper four accident management strategies for BWRs are analyzed:

EGG-RAAM-11207, *Preliminary Review of the Accident Management Guidelines for Three PWR Owner's Groups*

NUREG/CR-6009, *Developing and Assessing Accident Management Plans for Nuclear Power Plants*

NUREG/CR-6056, *A Framework for the Assessment of Severe Accident Management Strategies*

NUREG/CR-6158, *Implications for Accident Management of Adding Water to a Degrading Reactor Core*

Sandia National Laboratory, *BWR Low Power and Shutdown Accident Sequence Frequencies Project - PHASE 1 - COARSE SCREENING ANALYSIS (DRAFT), Volume 1 - Internal Events Excluding Fire and Flood,* June 1991.

Sandia National Laboratory, *Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1,* April 1995.

These reports presents results of a "Phase 1" and "Phase 2" analyses that encompassed a coarse screening and full analysis of potential accidents that could occur at a boiling water reactor (BWR) while operating at other than full power. This coarse screening approach was adopted as a means of obtaining, in a relatively short period of time, some estimation of the potential for accidents during low power and shutdown conditions and some idea of the magnitude of the work necessary to perform a more detailed analysis of these operating states (this work lead to

the NUREG-CR-6143 report). This work details operation in off-power modes of operation and may be useful as a resource to determine management strategies following a reactor trip.

E. M. Dougherty, "Credibility and Uncertainty Associated with Accident Management Actions," *Reliability Engineering and System Safety*, 37, 1992, 45-55.

This paper describes a qualitative analysis of the uncertainties that pervade accident management strategies. They range from situational uncertainty to human performance.

E. Daugherty, "EOPs, A Lingering Concern", Letter to the editors, *Reliability Engineering and System Safety*, 48, (1995), 235-238, 1995.

This paper presents interesting observation and issues to be addressed in accident management. These issues include: who is the decision maker; what form should emergency operating procedures have; how is it possible to make an efficient coordination between the inside and outside of the control room; and the ergonomics of EOPs. Note that these issues are just raised, not answered in this paper.